(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2001 (12.07.2001)

PCT

(10) International Publication Number
WO 01/49369 A1

(51) International Patent Classification[7]: A61N 1/372, A61B 5/117

(21) International Application Number: PCT/US00/35544

(22) International Filing Date:
29 December 2000 (29.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/173,822 30 December 1999 (30.12.1999) US

(71) Applicant: MEDTRONIC, INC. [US/US]; 7000 Central Avenue Northeast, Minneapolis, MN 55432 (US).

(72) Inventors: NICHOLS, Timothy, J.; 915 James Street, Lino Lakes, MN 55014 (US). THOMSON, David, L.; 14171 Alder Street Northwest, Andover, MN 55304 (US).

(74) Agents: WOLDE-MICHAEL, Girma et al.; Medtronic, Inc. MS 301, 7000 Central Avenue Northeast, Minneapolis, MN 55432 (US).

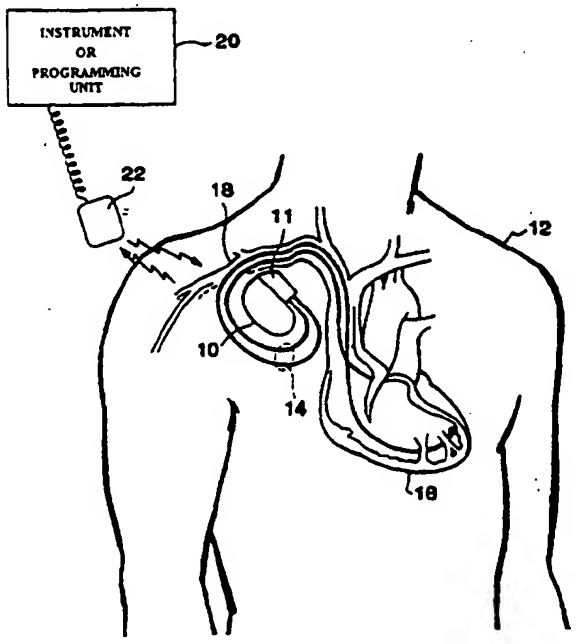
(81) Designated States *(national)*: CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *With international search report.*
— *With amended claims and statement.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: USER AUTHENTICATION IN MEDICAL DEVICE SYSTEMS



(57) Abstract: A user authentication system utilizes biometric traits such as fingerprints, vein print, voice print, facial images, iris/retina and similar distinguishing characteristics to allow access to programmers, PSAs, ETPs, and similar instruments associated with implantable medical devices (IMDs). The authentication system provides a hierarchical scheme that allows access based on expertise and need basis.

WO 01/49369 A1

USER AUTHENTICATION IN MEDICAL DEVICE SYSTEMS

FIELD OF THE INVENTION

The present invention generally relates to medical device systems. Specifically, the invention relates to biometric-based identification systems to provide a hierarchy of authorized access to operational hardware and software tools in medical devices. The biometric data may represent iris/retina, fingerprint, voiceprint, facial, veinal and similar biometric identification traits of individuals. These are stored in a database to confirm identification of an authorized person based on a correspondingly comparative code assigned to the biometric traits of a specific user. The identification code may be implemented in instruments such as a programmer, pacing system analyzer (PSA), external temporary pacemaker (ETP), home monitor and other peripheral units that are in data communication with implanted devices in a patient. Access to specific therapy and diagnostic tools and content are based on the hierarchy of authorization such as, for example, a doctor, a nurse, a patient, or a Medtronic employee, each of which would have qualified access granted with respect to their expertise and need basis.

BACKGROUND OF THE INVENTION

Medical devices, particularly implanted medical devices, require occasional and at times, chronic adjustments based on therapy and diagnostic needs of the patient. The therapy and diagnostic parameters that need adjustments may involve the decisions of doctors, nurses, Medtronic field service personnel, patients, members of the patient's family or representative, as the case may be. Further, the parameters to be adjusted, or the software to be implemented, in a medical device via an instrument such as a programmer or instruments, would require various levels and hierarchies of expertise. Misadjustment of the parameters could endanger the patient's life. Accordingly, there is need to limit access to these instruments to primarily protect the patient's privacy and well being.

Therapy regimen,and chronic patient and care treatment, via implanted medical devices would require timely decisions by physicians qualified to assess the

patient's conditions and dispense proper medical care. Further, implanted medical devices (IMDs) must be monitored on a regular or chronic basis to make adjustments of certain parameters or settings responsive to changes in a patient's condition or based on factors internal to the IMD. IMDs may also contain logic devices such as digital controllers which may need to undergo firmware or software upgrades or modifications. Further, various users, including doctors, nurses, Medtronic field personnel and the patient, may occasionally want to review physiologic data or patient information stored in IMDs to evaluate the performance of the device and review patient history as needed. Current practice provides operations in which software and instructions installed in an IMD could be modified responsive to patient diagnostic and therapeutic conditions.

Instruments such as programmers, PSAs, ETPs and similar devices are becoming ubiquitous. Specifically, as the segment of the population with IMDs increases, health care cost management would require various home monitors and instruments to be available at the disposal of patients for managing the operations of the IMDs, either by the patients, nurses or doctors, as the case may be. For example, the patient may be remotely instructed to adjust certain parameters without intervention of the physician. Similarly, in the case of a chronic patient, a nurse may be assigned to visit the individual at home so that the nurse may make qualified decisions to adjust or modify the operations of the IMD based on a review of diagnostic and therapeutic parameters retrieved from the device. While empowering patients and other qualified personnel is a viable economic option to reduce the cost of health care, user verification, user authorization and access control will clearly be needed to provide a secure and safe management of implanted devices in patients. Specifically, all peripheral and major devices that are used in downlinking to the IMD may potentially be a source of security and privacy breach unless protected by a security system.

There are several user authentication systems. Specifically, some implement biometric identification to control access to customize computer systems data. For example, some computers require fingerprint data to access users' sensitive information.

In this regard, PCT publication WO2000/22581 to Bromba, M., discloses an identification device with a sensor having an authentication surface with biometric features. A comparator compares detected biometric features of a part of the authentication surface of an authorized person or persons to determine the relative position of the sensor detected biometric features within the authentication surface. The computing device then computes an identification code which identifies the person detected by the sensor.

Similarly, U.S. Patent No. 5,401,561 to Borus et al, discloses identification characteristics formed as optical markings with radiation provided by a light source. The marking is in an optically transparent housing or surface or other area for at least a part of the wavelength range within the sensitivity range of the human eye and for a further part outside the human eye sensitivity range.

PCT publication WO2000/43960 to Frischholz, R., discloses a recognition system that is based upon medical data, obtained for example, from fingerprints or eyes. The method involves acquisition of data by scanning with a camera, for comparison with reference data. In order to prevent misuse, the reference data is based upon several samples from different positions. The user has to move a hand or eyes to form an object on the screen that would provide adequate data input to the controller. Similarly, PCT publication WO2000/021021 to Frischholz, R., discloses a face detecting system in which the images of a face model could be generated for identification purposes.

PCT publication WO2000/026823 to Garfinkle, N., discloses an individual medical record protection method for protecting medical records prepared in a doctors office or hospital. Specifically, the invention relates to a process by which a person authorized by the patient inputs personal identification and biometric codes to a database that checks if the biometric and Id number are in accord with that stored in the database. Upon confirmation, access is granted to a particular record that uses the Id code and the data is transmitted to the requesting site.

Accordingly, the use of biometrics for identification and authorization of users based on data associated with a stored key is well known in the art. However, the implementation of biometric recognition systems to enable access to instruments in

data communication with IMDs, presents new and non-obvious biometric implementation. Specifically, the implementation of biometric recognition systems to provide a layered and hierarchal access to instruments and IMDs on expertise and need, reduces opportunities for tampering, manipulation, error and harm to the patient. Accordingly, it is preferable to provide specific access to IMDs via instruments such as programmers, PSAs and other instruments, home monitors and programmers to doctors, nurses, Medtronic technicians and patients or patients' representatives, to enable safe monitoring and content specific adjustment or modifications of implanted medical devices.

SUMMARY OF THE INVENTION

The present invention provides a system for selective implementation of biometric user and instrument identification that enables secure and accurate data transfer between IMDs and instruments such as programmers. Embodiments of suitable biometric user authentication systems include, for example, user identification and password schemes, a scan of written signatures, biometric identification based on retina/iris or other unique body features, voice recognition, fingerprints, vein prints and similar biometric recognition traits hereinafter referred to as "biometric traits".

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a body implanted device system in accordance with the present invention, including an instrument such as a programmer in wireless data communication with the implanted medical device.

Figure 2 is a perspective view of an external programming unit. The invention utilizes the biometric traits to insure the identity of users. Further, the system enables segregated access to certain tools, text and operations based on the user's expertise, need and qualifications. For example, physicians have a broad-based access to therapeutic and diagnostic tools compared to nurses, technicians or the patients.

Figure 3 is a perspective view of an external programming unit with biometric recognition systems implemented therein.

Figure 4 is a perspective view of an external programming unit, such as an ETP, the biometric recognition system implemented therein.

Figure 5 is a flow chart of one embodiment of the user authentication process in accordance with the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of an implantable medical device (IMD) system adapted for use in accordance with the present invention. The medical device system of Figure 1 includes an IMD 10 implanted in patient 12. In accordance with conventional practice in the art, IMD 10 is housed within a hermetically sealed, biologically inert outer casing which may be conductive, to serve as an indifferent electrode in the IMD's pacing/sensing circuit. One or more pacemaker leads collectively identified with reference numeral 14 in Figure 1 are electrically coupled to IMD 10 in a conventional manner and extend into the patient's heart 16 via vein 18. Disposed generally near the distal end of leads 14, are one or more exposed conductive electrodes for receiving electrical cardiac signals and/or for delivering electrical pacing stimuli to heart 16. As will be appreciated by those of ordinary skill in the art, leads 14 may be implanted with each distal end situated in the atrium and/or ventricle of heart 16. Although the present invention will be described herein referring to this one embodiment which includes IMD 10, those of ordinary skill in the art, in light of the present disclosure, will appreciate that the present invention may be alternately practiced in connection with numerous other types of IMDs.

Further referring to Figure 1, an instrument/external programming unit 20 is shown in wireless data communication with IMD 10. Instrument 20 includes a programming head 22 in accordance with conventional medical device programming systems for facilitating two way communication between IMD 10 and instrument 20. In many known implantable device systems, a programming head such as that depicted in Figure 1 is positioned on the patient's body over the implant side of the device such that one or more antennae within head 22 can send RF signals to, and receive RF signals from, an antenna disposed within the hermetic enclosure of IMD

10 or disposed within the connector block of IMD 10 in accordance with common practice in the art.

Figure 2 is a perspective view of instrument or programming unit 20 in accordance with the present invention. Generally, programmer 20 includes a processing unit (not shown in the figure) that, in accordance with the presently disclosed invention, is a personal computer type mother board, for example, computer motherboard including an Intel PentiumIII microprocessor and related circuitry such as digital memory. The details of design and operation of the programmer's computer system will not be set forth in detail in the present disclosure, as it is believed that such details are well known to those of ordinary skill in the art.

Further, referring to Figure 2, programmer 20 comprises an outer housing 60 which is preferably made of a thermal plastic or equivalent rugged yet relatively lightweight material, and a carrying handle 62 integrally formed into the front of housing 60. Handle 62 is retractably designed to serve as a handle so that programmer 20 can be carried like a briefcase. An articulating display screen 64 is disposed on the upper surface of housing 60. Display screen 64 folds down into a closed position (not shown) when programmer 20 is not in use, thereby reducing the size of programmer 20 and protecting the display surface of display 64 during transportation and storage thereof.

As would be appreciated by those of ordinary skill in the art, it is often desirable to provide a means for determining the status of the patient's conduction system. This is generally accomplished by external ECG leads 24 which can provide suitable ECG tracings. Further, in accordance with the present invention, programmer 20 is equipped with an internal printer (not shown) so that a hard copy of a patient's ECG or graphics could be generated at display screen 64. Several types of printers such as AR 100 Printer from General Scanning Company are compatible with programmer 20.

Still referring to Figure 2, programmer 20 is shown with articulating display screen 64, having been lifted up into one of a plurality of possible open positions so that the display area thereof is visible to users situated in front of programmer 20. Articulating display screen is preferably of the LCD or electro luminous type

characterized by being relatively thin, as compared, for example a CRT or the like. As would be appreciated by those with ordinary skill in the art, display screen 64 is operatively coupled to the computer circuitry, disposed within housing 60, and is adapted to provide a visible display of graphics and/or data under control of the internal computer.

Programmer 20 as illustrated herein with reference to Figure 2 is substantially disclosed and described in more detail in U.S. Patent No. 5,345,362 to Thomas J. Winkler, entitled "Portable Computer Apparatus with Articulating Display Panel", which patent is incorporated herein by reference in its entirety. The Medtronic Model 9790 Programmer is the implantable device programming unit with which the present invention may be advantageously practiced.

Figure 3 is a perspective view of programming unit 20 incorporating the biometric identification systems in accordance with the present invention. Specifically, biometric sensor 70 for detecting fingerprints includes an area adapted to fit the front part of a user's finger. Similarly, microphone 72 is implemented on panel 64 to enable voice recognition. Further, camera 74 is implemented to enable reading of facial and other bodily features including iris/retina scans.

Figure 4 is a perspective view of ETP 80. Generally, ETP 80 is a mode switching apparatus for an external dual chamber cardiac pacemaker having multiple single chamber and dual chamber primary pacing modes and user adjustable atrial and ventricular sensitivities. The dual chamber demand pacing mode, for example, the DDE or DDI mode, is in effect as long as the atrial and ventricular pace pulse amplitudes are set by the user within an operative range. The pacing mode is switched to a single chamber demand mode when one of the atrial and ventricular pace pulse energies is set to an inoperative setting, which preferably is a no output setting. If the atrial pace pulse amplitude is set to no output, then the mode is switched to a single chamber demand mode with ventricular sensing and pacing, preferably the VVI mode. If the ventricular pace pulse amplitude is set to no output, then the mode is switched to a single chamber mode with atrial sensing and pacing, preferably the AAI mode. In the implementation of ETP 80, the setting of atrial or ventricular pace pulse amplitude to the off position is detected and the corresponding

atrial or ventricular sense amplifier is effectively rendered inoperative resulting in the mode switch. The mode switch back to the dual chamber demand pacing mode is affected by setting the atrial or ventricular pace pulse amplitude to any level other than the no output position. Preferably, the mode switch is to the DDD mode, even if the preceding mode switch was from the DDI mode.

ETP 80 described herein with reference to Figure 4 is substantially disclosed in more detail in U.S. Patent No. 5,626,621 to Skoglund et al, entitled "Dual Chamber Multi-Mode External Pacemaker" , which patent is incorporated herein by reference in its entirety. ETP 80 includes sensor 82 for detecting fingerprints, sensor 86, which includes a camera, to sense biometric data representing images and/or the iris and microphone 84 for collecting biometric data representing voiceprint and voice recognition systems.

Figure 5 is a flow chart of one embodiment of the user identification and authorization process 500 in accordance with the present invention. Specifically, when a user attempts to gain access to IMD 10, programmer 20 or ETP 80, the user enters appropriate authentication data at step 501. The identification data may include a fingerprint, an image, iris scan, voiceprint, or similar biometric traits. The system analyzes the input by preferably comparing it with stored data. If a match is confirmed, access is granted based on the authorization level to access specific tools and features of programmer 20, IMD 10 or ETP 80, as the case may be. Specifically, if authorization is confirmed, and access is authorized as shown at logic step 506, then step 516 determines the type of access and level under the authorization scheme for the specific user based on content, class or category assigned to the user as appropriate. For example, step 520 illustrates a third user or an untrained user who may have only limited usage/access rights such as no access to programmable operations or patient data. Step 522, however, may permit broader access such as perhaps are afforded to a doctor. Further, a nurse of appropriate identification may be granted access to limited programmable operations relating to diagnostic and therapy tools. Similarly, a patient user may be authenticated to access a limited set of tools that may be permitted to adjust non-critical settings. Furthermore, a Medtronic field representative may be allowed to access only operational/functional aspects that relate

to data collection and/or software upgrades, with strict limitations to any or all therapy and diagnostic tool adjustments. Alternatively, step 524 might be identified with the user's authentication and authorization category, and it may equate to that of a trained specialist. For example, this authorization may relate to someone who is authorized for access to programmable operations, patient data or other rights. Step 530 designates an end to the authorization sequence of a session. Logic pathway 504 represents the denial of user access. However, in this scenario, step 507 queries whether the user is requesting access in view of a special override function or emergency situation. If not, then the authentication is denied at step 509. In the event the special override function is approved, then logic pathway 511 routes the user to step 524. As indicated hereinabove, step 524 is normally identified with the user's identification and authorization category relating to a trained specialist and may provide a broad-based access to diagnostic, therapeutic and operational/functional features of programmer 20, IMD 10 and ETP 80.

It should be recognized that Figure 5 is merely one embodiment of a number of authentication schemes and logic systems enabled and claimed by this invention disclosure. Indeed, authentication system 500 may include combinations of hardware and software elements suitable for interface with the various instruments such as programmers, ETPs, PSAs and home monitors, to provide authorized access to these devices using the biometric identification system disclosed herein.

As indicated hereinabove, biometric data or traits used to authenticate and verify users may include retina or iris scans, fingerprint scans, vein print scans, voice prints, or voice recognition system, special geometry/facial recognition, hand geometry, veinal scans, and similar other biometric traits and features that could be used to positively identify a user. The authentication techniques implemented in the present invention include hierarchical schemes of grant to primary, secondary and occasional users. For example, doctors and nurses could be considered primary users, having access to specific therapeutic and diagnostic tools, both instruments and IMDs.

In addition to the various biometric techniques disclosed in the present invention, instrument and IMD related authentication mechanisms may include verification through use of; inscription techniques, approved serial numbers, fixed or

pre-loaded data signatures in the instrument or IMD memory, resistance or other electrical or digital characteristic matching, load recognition, or data message generated by one or more predetermined algorithm based on dates, events, serial number or other phenomenon.

Referring now to Figures 3 and 4, the implementation of the various biometric identification systems in programmer 20 and ETP 80, include voice recognition via microphone 72 and 84 respectively, face recognition or iris scan using camera 74 or 86 respectively, and fingerprint recognition using fingerprint sensors 70 and 82 respectively. The iris scan and face recognition biometric systems may be the type manufactured by Iris Scan, Inc., Symtron Technology, Dialog Communication Systems, Visionics Corp. Further, biometric fingerprint sensors may be of the type supplied by Miaxis Biometrics Co., Advanced Biometric Solutions, Veridicon Face Sense, and Precise Biometrics. Further, voice recognition systems for voice print identification may be of the type offered by Dialogue Communication Systems.

Accordingly, the biometric identification systems contemplated by the present invention may be implemented from various suppliers for incorporation in programmer 20, ETP 80 and similar instruments. One of the significant aspects of the present invention includes the implementation of biometric data to eliminate error, tampering and provide patients with a high level of security to maintain medical data privacy.

Although the invention is described with reference to particular embodiments, it will be understood to those skilled in the art that this embodiment is merely illustrative of the application of the principles of the invention. Numerous modifications may be made therein, and other arrangements may be devised without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A user recognition system to identify a user and enable access to instruments associated with at least one implanted medical device, the system comprising:

an implanted medical device in a patient;

an instrument in data communications with the implanted medical device; and

the user recognition system for submitting biometric traits of the user implemented in said instrument.

2. The system of claim 1 wherein said implanted medical device includes one of a pacer, a defibrillator, a drug delivery device and a neural implant.

3. The system of claim 1 wherein said instrument includes one of a programmer, a PSA and a home monitor.

4. The system of claim 1 wherein said user recognition system includes at least one of a finger scanner, a camera and a microphone.

5. The system of claim 4 wherein said biometric traits include a finger scan obtained from said finger scanner.

6. The system of claim 4 wherein said biometric traits include an iris/retina scan obtained via said camera.

7. The system of claim 4 wherein said biometric traits include a voice print obtained from said microphone.

8. A biometric-based user authentication system for identifying and granting access to at least one user to an implanted medical device in a patient associated with an instrument, the authentication system comprising:

at least one biometric sensor implemented in the instrument;

at least one biometric trait of a user stored as coded data in a memory bank of said biometric sensor; and

means for analyzing and comparing said at least one biometric trait with said coded data to grant or deny access.

9. The system of claim 8 wherein said at least one biometric sensor includes at least one of a camera, a finger print sensor and a microphone.

10. The system of claim 8 wherein said at least one biometric trait of a user includes a fingerprint, a voice print, an iris/retinal print, a facial model, a veinal imprint and a digital signature.

11. The system of claim 8 wherein said means for analyzing and comparing includes a software system implemented in the memory bank of the biometric sensor.

12. The system of claim 8 wherein said biometric traits of a user stored as coded data includes instructions to allow a user with matching biometric traits to have access to a pre-determined set of data and tools of said implanted medical device.

13. A method for a biometric-based identification of a user to provide authorized access to operational hardware, software and paticnt medical data contained in instruments and implanted medical devices, the method comprising:

accepting at least one biometric trait from a potential user;

comparing said at least one biometric trait to a stored coded data; and

granting a qualified access when a match is confirmed between said at least one biometric trait and the stored coded data.

14. The method of claim 13 wherein said qualified access includes a hierarchical scheme to enable user-specific access and authorization based on expertise and need.

15. The method of claim 14 wherein said hierarchical scheme includes distinctions of access to various hardware, software tools to perform therapy, diagnostic and monitoring functions designed to provide various levels of authorized access to physicians, nurses, Medtronic technicians, patients and their representatives.

AMENDED CLAIMS

[received by the International Bureau on 06 July 2001 (06.06.01); original claims 1-15 replaced by new claims 1-5 (1 page)]

1. An external instrument operable in a data communications mode to establish a communication link with an implanted medical device in a patient, characterized in that access to data communications mode is controlled by a user authentication system for identifying an authorized user comprising:

a biometric trait sensor (70, 72, 74) providing coded data representative of the biometric trait of a potential user;

a memory storing coded data representative of biometric traits of authorized users to be granted access to the data communications mode of the instrument; and

an authorization analyzer comparing coded data from the biometric trait sensor with the coded data stored in the memory to determine whether a potential user is authorized to have access to the data communications mode of the external instrument.

2. The instrument of claim 1 wherein data communication comprises programming data for establishing operation of the implanted medical device.

3. The instrument of claim 1 wherein the biometric trait sensor is selected from a group consisting of a fingerprint scanner for a fingerprint scan, a camera for an iris/retina scan, and a microphone for a voiceprint scan.

4. The instrument of claim 1 wherein the memory further stores coded data for each authorized user that includes a hierarchical scheme to enable user-specific access and authorization based on expertise and patient need.

5. The instrument of claim 4 wherein said hierarchical scheme includes distinctions of access to various hardware, software tools to perform therapy, diagnostic and monitoring functions designed to provide various levels of authorized access to physicians, nurses, technicians, and patients.

PRELIMINARY AMENDMENT AND STATEMENT UNDER ARTICLE 19(1)

Statement Under Article 19(1):

The amendments provided by new claims 1-5 do not have any impact on the description or the drawings.

The difference between the new claims 1-5 being presented and the original claims is that the subject matter of the invention is set forth in a more concise fashion and emphasizes that a biometric trait based user authentication system is provided for identifying an authorized user to have access to communications with an implanted medical device.

The new claims 1-5 distinguish from the subject matter disclosed in the references cited in the International Search Report in that none of the citations discloses biometric trait based user authentication system.

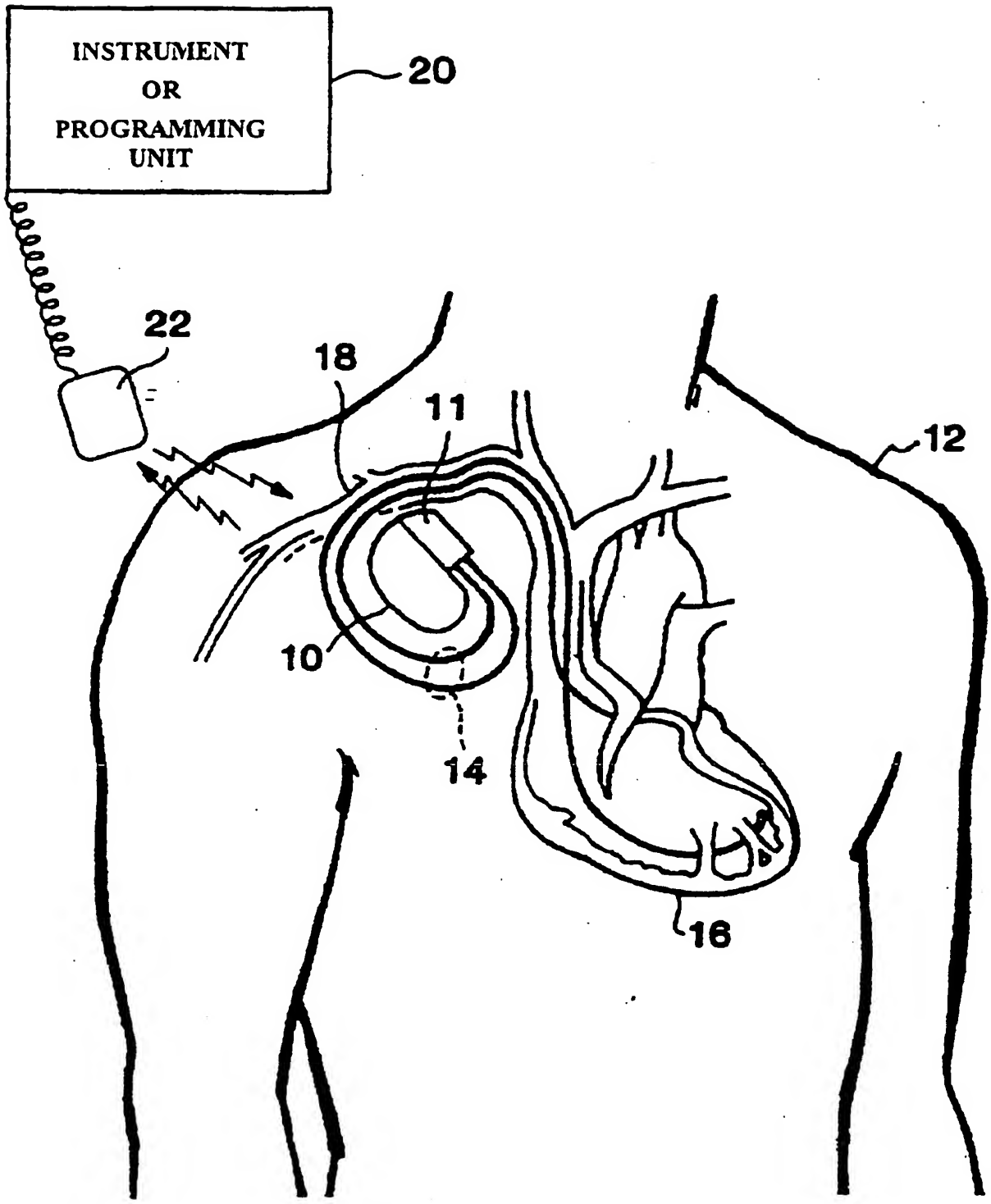


Figure 1

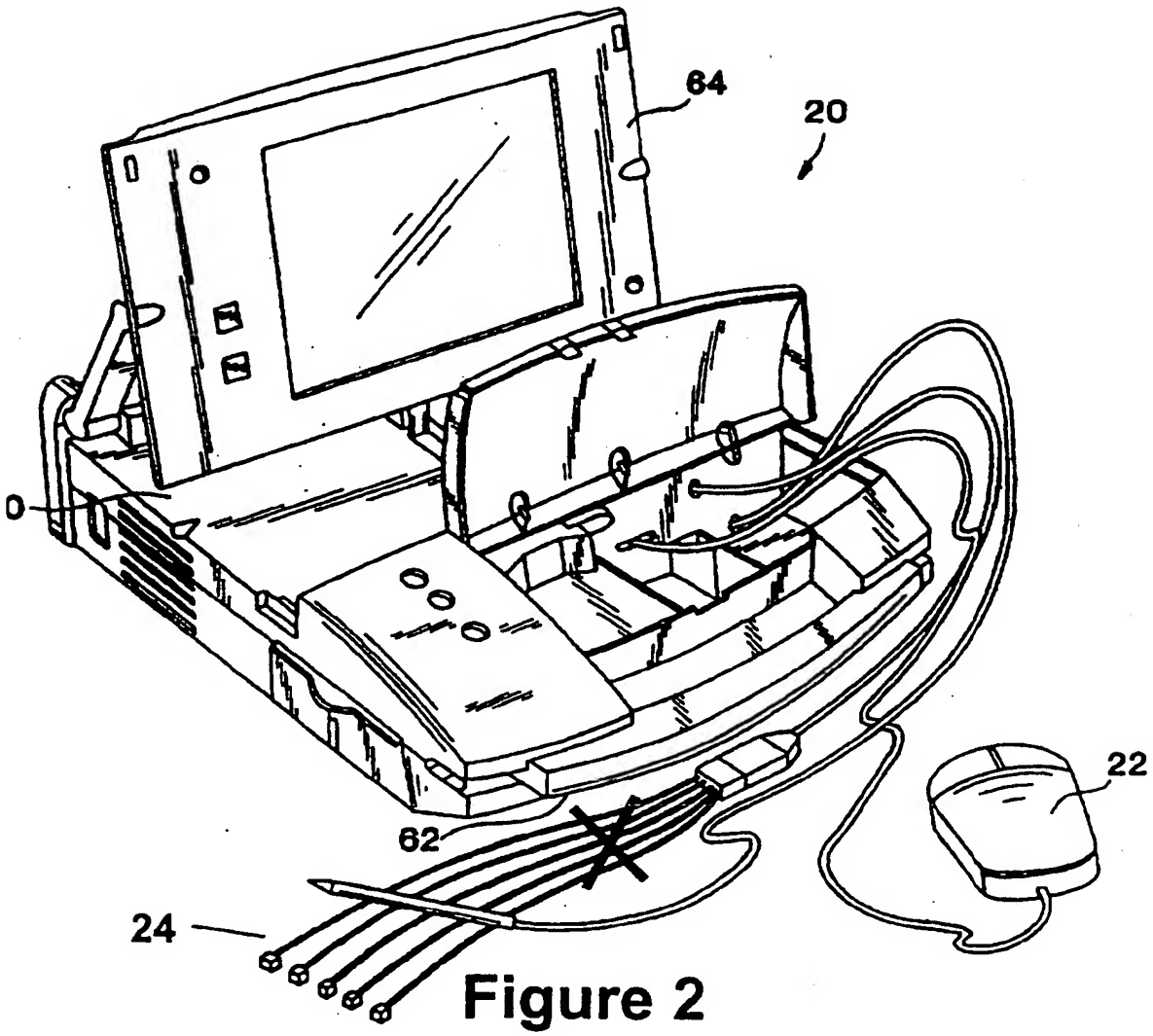


Figure 2

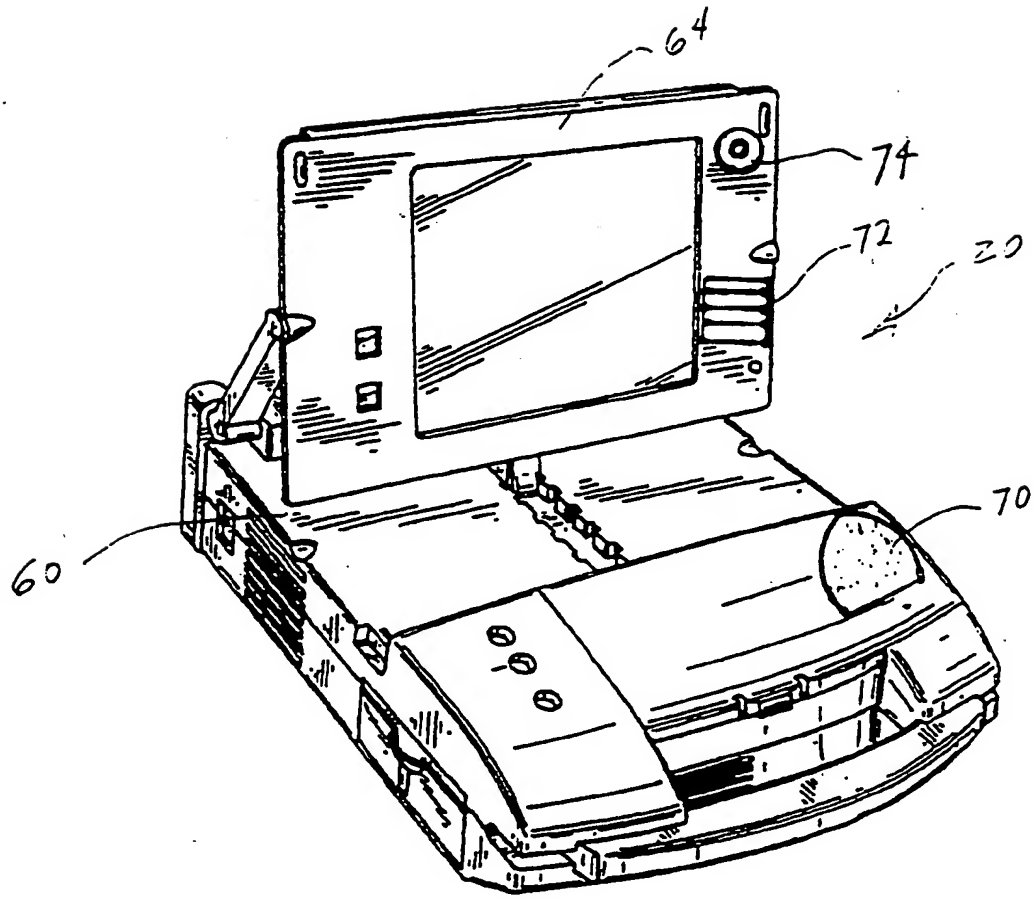


Figure 3

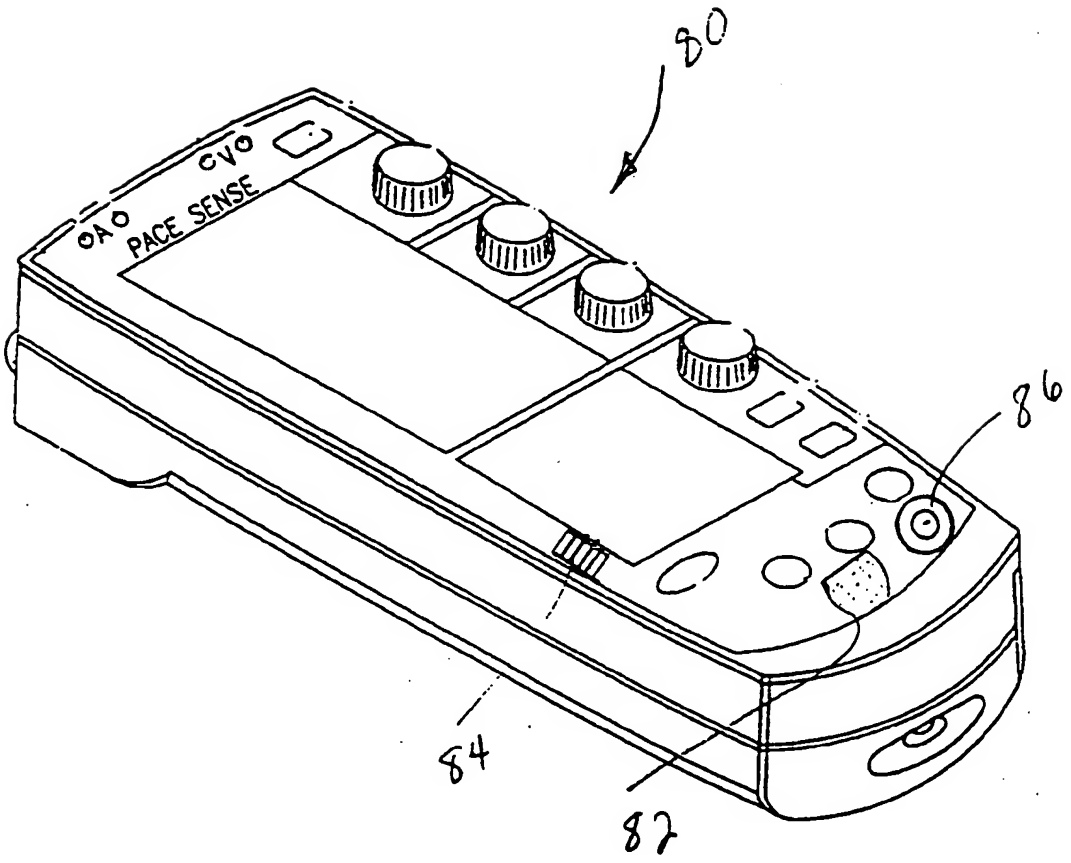


Figure 4

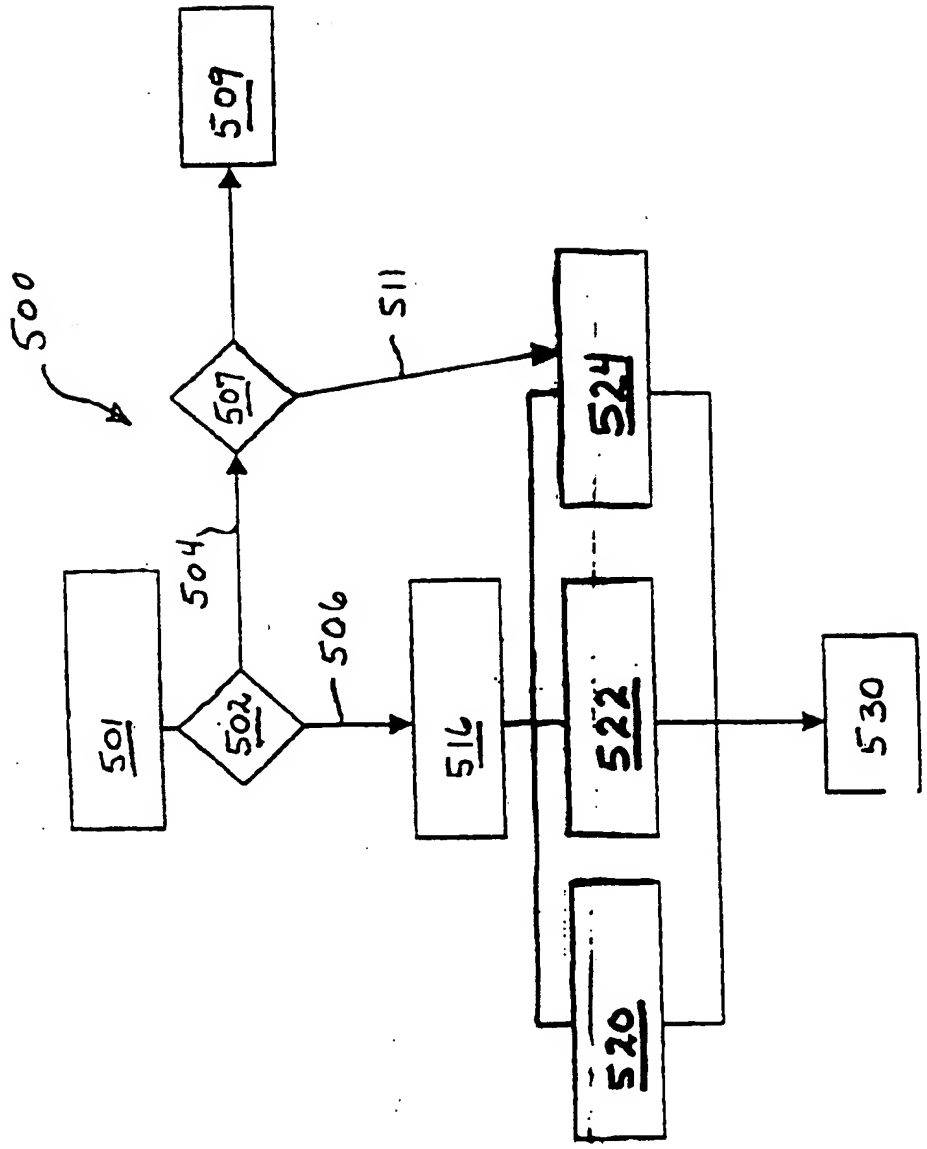


Figure 5

INTERNATIONAL SEARCH REPORT

In. ational Application No
PCT/US 00/35544

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 A61N1/372 A61B5/117

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 A61N A61B G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 456 692 A (SMITH JR ROBERT E ET AL) 10 October 1995 (1995-10-10) column 9, line 5 - line 46 column 11, line 28 - line 68; claims	1-15
Y	US 5 838 306 A (O'CONNOR CLINT ET AL) 17 November 1998 (1998-11-17) column 1, line 13 -column 2, line 25 abstract; claims	1-5,8-13
Y	US 4 432 360 A (MUMFORD VAN E ET AL) 21 February 1984 (1984-02-21) column 2, line 41 -column 3, line 15 column 22, line 59 -column 23, line 15; claims	14,15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 April 2001	06/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Manschot, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/US 00/35544

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 229 764 A (KEHOE BRIAN D ET AL) 20 July 1993 (1993-07-20)	1-15
Y	column 1, line 44 -column 2, line 32	6,7

INTERNATIONAL SEARCH REPORT

Information on patent family members

In .ational Application No
PCT/US 00/35544

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5456692 A	10-10-1995	NONE	
US 5838306 A	17-11-1998	NONE	
US 4432360 A	21-02-1984	DE 3225223 A	03-03-1983
		FR 2512987 A	18-03-1983
		JP 58103469 A	20-06-1983
US 5229764 A	20-07-1993	NONE	